4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,785	06/29/2001	Kenji Ohkuma	210580US2SRD	4586

22850 7590 02/28/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/893,785	**Applicant(s)** OHKUMA ET AL.
	Examiner Zachary A Davis	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *20010629, 20040112*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

2. Claims 5, 6, 12, and 13 are objected to because of the following informalities:

Claims 5 and 6 each recite the limitation "comprises a first-half second nonlinear transformation units" in lines 3-4 of each claim. It appears that either "a" should be deleted or "units" should be changed to read "unit".

Applicant is advised that should claim 5 be found allowable, claim 6 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim 12 recites the limitation “a third nonlinear transformation units” in lines 23-24 of page 82. It appears that either “a” should be deleted or “units” changed to “unit”. Further, in line 26 of page 82, it appears that in the limitation “each of the first diffusion unit”, “unit” should be changed to “units”. Additionally, it appears that the limitation “corresponding bits positions” in lines 6-7 of page 83 should read “corresponding bit positions”.

Claim 13 recites the limitation “a third nonlinear transformation units” in lines 16-17 of page 85. It appears that either “a” should be deleted or “units” changed to “unit”. Further, in line 19 of page 85, it appears that in the limitation “each of the first diffusion unit”, “unit” should be changed to “units”. Additionally, it appears that the limitation “corresponding bits positions” in lines 26-27 of page 85 should read “corresponding bit positions”.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 9-10 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least one bit of data input to the first unit in own encrypting section being transmitted to at least one bit of data input to the first unit in the succeeding encrypting section via at least two routes" is generally vague. Specifically, it is not clear how a bit is transmitted to another bit, nor is it clear how the bit is transmitted by more than one route.

Claim 2 recites the limitation "the at least one bit". It is unclear whether this refers to the "at least one bit of data input to the first unit in own encrypting section" or to the "at least one bit of data input to the first unit in the succeeding encrypting section". This renders the claim indefinite.

Claim 3 recites the limitation "for some of the combinations" in line 6 of the claim. This renders the claim indefinite, as it is unclear exactly what numerical range is encompassed by the term "some". Further, the limitation "one bit of the data input to the first unit in the own encrypting section is transmitted to one bit of the data input to the first unit in the succeeding encrypting section via at least two routes" is generally vague. Specifically, it is not clear how a bit is transmitted to another bit, nor is it clear how the bit is transmitted by more than one route.

Claim 4 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 12-13 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least one bit of data input to one of the second nonlinear transformation units in each of the encrypting sections is transmitted to at least one bit of data input to one of the second nonlinear transformation units in the succeeding encrypting section via at least two routes" is generally vague. Specifically, it is not clear how a bit is transmitted to another bit, nor is it clear how the bit is transmitted by more than one route.

Claims 7 and 8 each recite the limitation "changing a bit extracted position" in lines 8-9 of each claim. It is generally unclear how the bit position is changed, or to what it is changed.

Claim 10 recites the limitation "the Galois field". There is insufficient antecedent basis for this limitation.

Claim 12 recites the limitation "comprising four first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of four sets of 32-bit data into which 128-bit block data is divided" in lines 15-20 of page 81. This limitation is generally unclear, especially the phrase beginning "a corresponding one". Further, the claim recites the limitation "four first nonlinear transformation units" in both lines 15-16 and 27 of page 81; it is unclear whether these refer to the same units. Similarly, the use of the limitation "the four first nonlinear transformation units" in lines 5-6 of page 82 and in lines 22-23 and 25-26 of page 83 renders the claim indefinite because it is not clear to which of the units on the preceding page this refers. Additionally, the use of the phrase "or its equivalent circuit" in lines 5 and 19 of page 83 renders the claim indefinite because the claim includes elements not actually disclosed, thereby rendering the scope of the claim unascertainable. Still further, the limitation "taken as one element" in lines 10 and 15 of page 83 is generally vague. Finally, the limitation of page 83, line 17-page 84, line 2, beginning "in the 4 x 4 matrix" is generally vague, especially the phrase "transmitting... the state of that one bit in the preceding stage to that one bit in the succeeding stage is transmitted". The use of the limitation "that one bit" is unclear, as it cannot be determined whether the limitation refers to the "one bit" of line 20 or of line 24 (on page 83), nor is the use of the limitation "the state of that one bit in the preceding stage to that one bit in the succeeding stage is transmitted over a plurality of operations paths" clear. Specifically, it is not clear how a bit is transmitted to another bit, nor is it clear how the bit is transmitted by more than one route.

Claim 13 recites the limitation "comprising two first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of two sets of 32-bit data into which 64-bit block data is divided" in lines 9-13 of page 84. This limitation is generally unclear, especially the phrase beginning "a corresponding one". Further, the claim recites the limitation "two first nonlinear transformation units" in lines 9-10 of page 84, and "four first nonlinear transformation units" in line 20 of page 84; it is unclear whether the two are included in the four units. Additionally, the use of the phrase "or its equivalent circuit" in line 25 of page 85 and line 12 of page 86 renders the claim indefinite because the claim includes elements not actually disclosed, thereby rendering the scope of the claim unascertainable. Still further, the limitation "taken as one element" in lines 3 and 8 of page 86 is generally vague. Finally, the limitation of page 86, lines 10-22, beginning "in the 2 x 2 matrix" is generally vague, especially the phrase "transmitting... the state of that one bit in the preceding stage to that one bit in the succeeding stage is transmitted". The use of the limitation "that one bit" is unclear, as it cannot be determined whether the limitation refers to the "one bit" of line 13 or of line 16 (on page 86), nor is the use of the limitation "the state of that one bit in the preceding stage to that one bit in the succeeding stage is transmitted over a plurality of operations paths" clear. Specifically, it is not clear how a bit is transmitted to another bit, nor is it clear how the bit is transmitted by more than one route.

Claim 14 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 4-6 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least two bits of the randomized data is reflected on one bit of data to be randomized next" in lines 8-9 of the claim is generally vague, as it is unclear exactly how the bits are "reflected".

Claim 15 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 8-10 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least two bits of the randomized data is reflected on one bit of data to be randomized next" in lines 13-14 of the claim is generally vague, as it is unclear exactly how the bits are "reflected".

Claim 16 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 9-10 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least one bit of data input to the first unit in own encrypting section being transmitted to at least one bit of data input to the first unit in the succeeding encrypting section via at least two routes" is generally vague. Specifically, it is not clear how a bit is transmitted to another bit, nor is it clear how the bit is transmitted by more than one route.

Claim 17 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 5-7 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least two bits of the randomized data is reflected on one bit of data to be randomized next" in lines 9-10 of the claim is generally vague, as it is unclear exactly how the bits are "reflected".

Claim 18 recites the limitation "with respect to a range which is wider than a range of the first subblock data" in lines 8-10 of the claim. It is unclear exactly what is meant by "range" in this limitation, and what type of measure is encompassed by the term, which renders the claim indefinite. Further, the limitation "at least two bits of the randomized data is reflected on one bit of data to be randomized next" in lines 13-14 of the claim is generally vague, as it is unclear exactly how the bits are "reflected".

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-9, 11, and 14-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Delayaye et al, US Patent 4751733.

In reference to Claims 1-3, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes a unit to randomize subblock data obtained by dividing block data and a unit to diffuse data output from the randomizing unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5).

In reference to Claim 4, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes a first nonlinear transformation unit and a first linear diffusion unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5). Delayaye further discloses that the first nonlinear transformation unit can include a second nonlinear transformation unit and a second linear diffusion unit (note that there are multiple permutation and substitution circuits in Figure 1; see also column 8, lines 12-37, particularly noting that it is possible to perform any number of possibly asymmetrical successions of substitution-permutations).

In reference to Claims 5 and 6, Delayaye further discloses that the second nonlinear transformation unit includes portions preceding and following the second diffusion unit (see column 8, lines 12-37, noting that the orders of operations can be changed and that operations can be carried out in several steps).

In reference to Claims 7 and 8, Delayaye further discloses dividing the blocks into subblocks of equal lengths (column 2, lines 20-32), and performing the linear diffusion process (see, for example, column 3, lines 50-63).

In reference to Claims 9 and 11, Delayaye further discloses implementing the diffusion unit in hardware (note the memories in Figure 1) or software (the memories may be programmable, column 5, lines 54-56).

Claims 14 and 15 are directed to a method and a software implementation, respectively, of the apparatus of Claim 1, and are rejected by a similar rationale.

Claim 16 is directed to a decryption apparatus which merely performs the reverse function of the encryption apparatus of Claim 1, and is rejected by a similar rationale, further noting that Delayaye discloses that the same device may be used for enciphering and deciphering (column 3, lines 42-46). Claims 17 and 18 are directed to a method and a software implementation, respectively, of the apparatus of Claim 16, and are rejected by a similar rationale.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 10, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Delayaye in view of Matsui et al, US Patent 6201869.

In reference to Claim 10, Delayaye discloses everything as applied to Claim 9 above. However, Delayaye does not explicitly disclose that the diffusion unit is based on multiplication over a Galois field. Matsui discloses a block encryption apparatus that includes a diffusion unit based on operations over a Galois field (see, for example, column 8, lines 45-48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Delayaye by basing the diffusion unit on operations over a Galois field, in order to increase the speed of encryption (see Matsui, column 2, lines 4-8).

In reference to Claims 12 and 13, Delayaye discloses an apparatus for block encryption that includes a series of encrypting sections, each of which includes first nonlinear transformation unit and a first diffusion unit (see Figure 1, permutation circuits 1, 6, and 8, and substitution memories 2-5). Delayaye further discloses that the first nonlinear transformation unit can include a second nonlinear transformation unit and a second linear diffusion unit (note that there are multiple permutation and substitution circuits in Figure 1; see also column 8, lines 12-37, particularly noting that it is possible to perform any number of possibly asymmetrical successions of substitution-permutations, and further noting that the orders of operations can be changed and that operations can be carried out in several steps). Although Delayaye does not explicitly disclose the block sizes of 128 or 64 bits of Claims 12 and 13 respectively, Delayaye states that the block size may be changed (column 2, lines 20-32). Further, although Delayaye does disclose using the key in the substitution boxes (see Figure 1), Delayaye does not explicitly disclose key addition units. Delayaye also does not explicitly disclose the use of an operation based on multiplication over a Galois field.

Matsui discloses a block encryption apparatus that includes a diffusion unit based on operations over a Galois field (see, for example, column 8, lines 45-48). Matsui further discloses the use of key addition units (the key is used at the XOR circuits, column 8, lines 45-48). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Delayaye by basing the diffusion unit on operations over a Galois field and including the key addition units, in order to increase the speed of encryption (see Matsui, column 2, lines 4-8).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ritter, US Patent 5727062, discloses a block cipher that includes the use of a matrix for diffusion.

b. Luyster, US Patent 6182216, discloses a block cipher that includes permutation functions.

c. Kanda et al, US Patent 6769063, discloses a block cipher that includes linear and non-linear data transformations, diffusions, and permutations.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER